thalesgroup.com

THALES

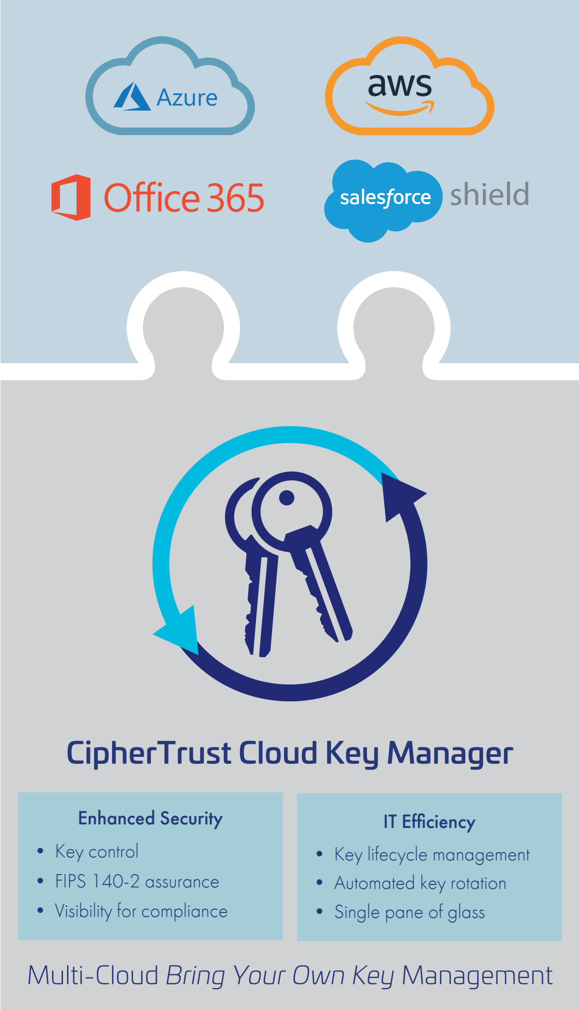
CipherTrust Cloud Key Manager

Many infrastructure-, platform-, and software-as-a-service providers offer data-at-rest encryption capabilities with encryption keys managed by the service provider. Meanwhile, many industry or internal data protection mandates, as well as industry best practices as defined by the Cloud Security Alliance, require that keys be stored and managed remote from the cloud service provider and the associated encryption operations. Providers can fulfill these requirements by offering "Bring Your Own Key" (BYOK) services to enable customer control of the keys used to encrypt their data. Customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them.

Leveraging cloud provider BYOK API's, the CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility.

Take control of your cloud encryption keys

- Leverage the value of "Bring Your Own Key" services with full-lifecycle cloud encryption key management
- Comply with the most stringent data protection mandates with up to FIPS 140–2 Level 3 validated key origination and storage
- Gain higher IT efficiency with centralized key management across multiple cloud environments, automated key rotation and key expiration management



CipherTrust Cloud Key Manager

Enhanced Security	IT Efficiency
Key control FIPS 140-2 assurance Visibility for compliance	Key lifecycle management Automated key rotation Single pane of glass

Multi-Cloud *Bring Your Own Key* Management

The key control imperative

The requirement to protect sensitive data across Infrastructure-, Platform-, and Software-as-a-Service (IaaS, PaaS, and SaaS) has resulted in broader cloud provider encryption offerings. Meanwhile the Cloud Security Alliance and industry analysts state that encryption keys should be held by customers. The challenges of holding keys grow with up to hundreds of master keys per subscription to be secured and managed across multiple clouds. There is also the imperative of knowing how, when, and by whom encryption keys are used. The CipherTrust Cloud Key Manager provides comprehensive key lifecycle management to fulfill requirements for safe, comprehensive key management across multiple clouds.

Supported clouds include:

- Microsoft Azure
- Microsoft Office365
- Microsoft Azure Stack
- Microsoft Azure China and Germany National Clouds
- Amazon Web Services
- Salesforce.com
- Salesforce Sandbox

Strong encryption key security

Customer key control presents requirements for secure key generation and storage. CipherTrust Cloud Key Manager leverages the security of the Vormetric Data Security Manager, SafeNet KeySecure, or supported hardware security modules (HSMs) to create keys and store them with FIPS 140–2 security. With the requirement for key security mechanisms such as safe storage of cloud backup keys, CipherTrust Cloud Key Manager acts as a key escrow for supported clouds and allows for full key metadata control both during upload and for keys in use.

Enhanced IT efficiency

CipherTrust Cloud Key Manager offers multiple capabilities in support of enhanced IT efficiency:

- Centralized Key Management gives you access to each cloud provider from a single browser window, including across multiple accounts or subscriptions
- Automated key rotation offers IT efficiency and enhanced data security
- Federated login provides a simple mechanism for granting access to key data. Cloud service logins are authenticated and authorized by the service provider—no login database nor AD or LDAP configuration is required
- For workloads that require it, CipherTrust Cloud Key Manager can request creation of native cloud provider keys and provide full lifecycle management for them
- With varying key technologies and terminology, CipherTrust Cloud Key Manager presents key operations in the semantics of the cloud provider
- Already created thousands of keys at your cloud provider? CipherTrust Cloud Key Manager will synchronize its database with keys created at the cloud provider

The compliance tools you need

CipherTrust Cloud Key Manager cloud-specific logs and prepackaged reports offer fast compliance reporting. Logs may also be directed to a syslog server or SIEM.

Implementation Choices that Match Your Needs

CipherTrust Cloud Key Manager offers several convenient implementation choices to meet your security and deployment needs:

- All-software is available with FIPS 140–2 Level 1-certified key security. The CipherTrust Cloud Key Manager Virtual Appliances and either the Data Security Manager or KeySecure virtual appliances can be instantiated in Amazon Web Services or Microsoft Azure, or deployed in any public- or private cloud leveraging VMware.
- Customer that require FIPS 140–2 Level 3 or 2 can deploy or utilize existing Vormetric Data Security Manager appliances or supported HSMs in on-premises or hosted data centers.

Multi-cloud data security solutions

CipherTrust Cloud Key Manager simplifies the need to hold and manage encryption keys for cloud services, a critical solution for fulfilling industry and organizational data protection mandates. Additional Thales multi-cloud security products, including Bring Your Own Advanced Encryption, all with centralized, FIPS-validated key management, enable you to encrypt and control cloud storage to reduce the chance of your sensitive data being leaked.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Thales solutions for Microsoft Azure

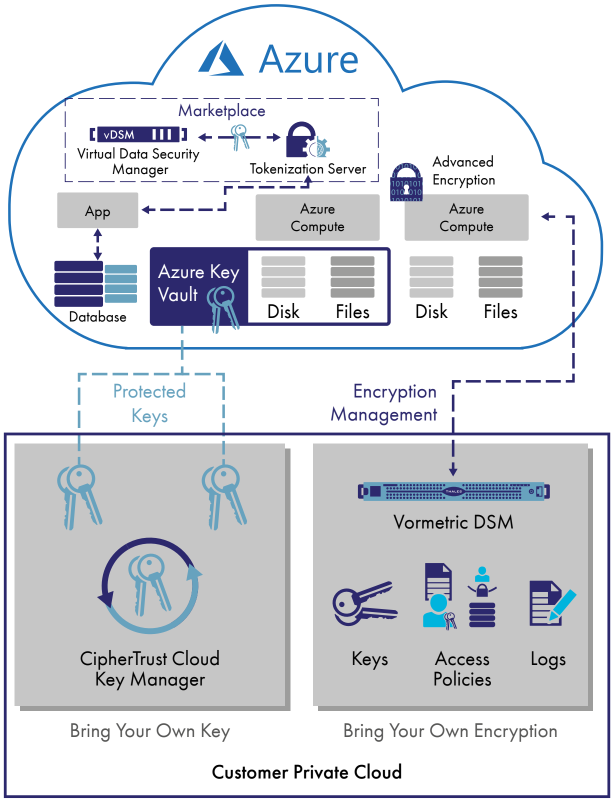
Secure workloads across hybrid clouds including Microsoft Azure

Information technology workloads in Microsoft Azure can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices, for protecting data. Further, you need rapid data mobility across all clouds you use and those in your future, a need which can be compromised with cloud-vendor-specific encryption solutions.

Advanced encryption with comprehensive key management

Effective, secure use of cloud services involves an increasing number of decisive moments, such as when you consider using sensitive data in any cloud. You can rely on Thales to secure your digital transformation. Thales advanced encryption and centralized key management solutions give you protection and control of data stored on your premises, Microsoft Azure, and other cloud providers. Thales technology enables you to:

- Avoid cloud vendor encryption lock-in and ensure the data mobility you need while you efficiently and securely spread workloads and data across multiple cloud vendors, including Microsoft Azure, with centralized, independent encryption management
- Take secure advantage of Azure Key Vault with centralized key management that spans multiple clouds
- Identify attacks faster with data access logging to industry-leading SIEM applications
- Reduce or eliminate risks arising from compromised credentials with advanced encryption including privileged user access controls
- Architect applications for the cloud with built-in security using vaultless tokenization with dynamic data masking



Advanced encryption for Microsoft Azure and beyond

If you're 100% Microsoft Azure-based with stringent data security controls, or if you're running hybrid clouds with data distributed across your on-premises private cloud, multiple cloud providers, and on Microsoft Azure, you need an advanced data encryption solution. Vormetric Transparent Encryption protects your files and databases stored anywhere, including Microsoft Azure, without any changes to applications, databases, infrastructure or business practices. Bring your own encryption to Microsoft Azure and other infrastructure as a service providers!

Vormetric Transparent Encryption:

- Strengthens data security with controls against unauthorized access based on granular access policies, including user identity (including for administrators with root privileges), and process, among many others
- Accelerates breach detection and satisfy compliance mandates with detailed file access logs directed to your security information and event management (SIEM) system
- Delivers a fast return on investment with a non-intrusive, flexible implementation. Encryption agents operate on Azure compute instances or any other server accessing storage, protect Azure Disk and Azure Files, and are available for many Windows versions and Linux distributions

Centralized, secure key management

The Vormetric Data Security Manager centralizes key, policy and log management for Vormetric Transparent Encryption, available as a FIPS 140-2 Level 2 or 3 appliance for on-premises deployment, or a FIPS 140-2 Level 1 instance on the Azure Marketplace.

Accelerated PCI-DSS compliance

Vormetric Tokenization with Dynamic Data Masking secures and anonymize sensitive assets in the data center, big data environments or the cloud for simplified PCI-DSS compliance. Format-preserving or random tokenization protects sensitive fields while maintaining database structure, for a non-disruptive implementation. Then, it's easy to add policy-based dynamic data masking to applications.

The Vormetric Tokenization Server is available on the Microsoft Azure Marketplace.

Multicloud encryption key management

Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using CipherTrust Cloud Key Manager.

The CipherTrust Cloud Key Manager leverages cloud provider Bring Your Own Key (BYOK) API's to reduce key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility. The solution is available on the Microsoft Azure Marketplace, or can be deployed on premises or in any private cloud deployment to meet more stringent compliance requirements.

CipherTrust Cloud Key Manager offers the following advantages:

- Safer key management practices combined with cloud benefits of scale, cost and convenience
- Greater control over keys—you can control key generation and storage of keys used in Microsoft Azure, Microsoft Azure Stack, Azure Government, Azure Germany and China National Clouds, AWS KMS, and more!
- Enhanced IT efficiency with multi-cloud key management from a single console that offers automated key rotation and comprehensive key life cycle management

Fulfill your data protection requirements

Thales simplifies securing your Microsoft Azure workloads and helps achieve compliance with data security regulations. Vormetric Transparent Encryption and Tokenization operate seamlessly on workloads in Microsoft Azure and on your premises delivering centralized policy and key management. And CipherTrust Cloud Key Manager brings you into compliance with best practices and data protection mandates pertaining to cloud key management.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com

thalescpl.com

THALES

Thales Solutions for Amazon Web Services

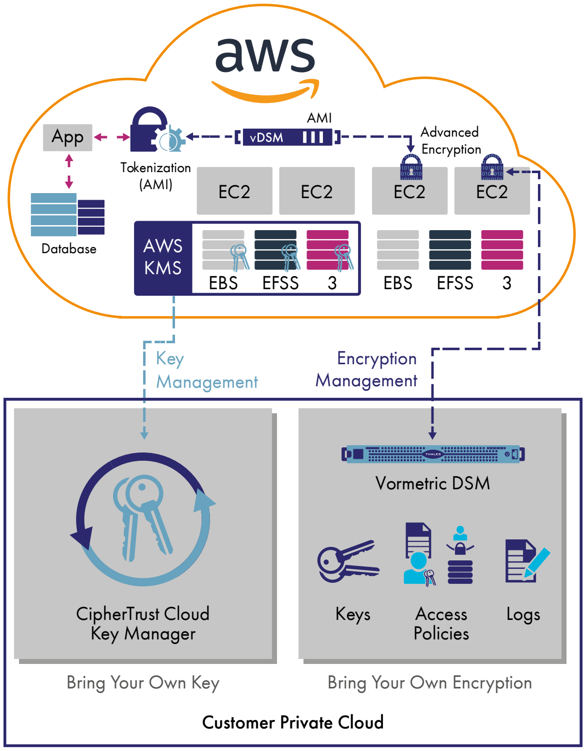
Secure workloads across hybrid clouds including Amazon Web Services

Information technology workloads in Amazon Web Services (AWS) can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices, for protecting data. Further, you need rapid data mobility across all clouds you currently use and those in your future, a need which can be compromised with cloud-vendor-specific encryption solutions.

Advanced encryption solutions with comprehensive key management

Effective, secure cloud use involves an increasing number of decisive moments, such as when you consider using sensitive data in any cloud. You can rely on Thales to secure your digital transformation. Thales advanced encryption and centralized key management solutions give you protection and control of data stored on your premises, Amazon Web Services, and other cloud providers. Thales technology enables you to:

- Avoid cloud vendor encryption lock-in and ensure the data mobility you need while you efficiently and securely spread workloads and data across multiple cloud vendors, including Amazon Web Services, with centralized, independent encryption management
- Take secure advantage of Amazon Key Management Services (AWS KMS) with a centralized key management solution that spans multiple clouds
- Identify attacks faster with data access logging to industry-leading SIEM applications
- Reduce or eliminate risks arising from compromised credentials with advanced encryption including privileged user access controls
- Architect applications for the cloud with built-in security using vaultless tokenization with dynamic data masking



Advanced encryption for Amazon Web Services and beyond

If you're 100% Amazon Web Services-based with stringent data security controls, or if you're running hybrid clouds with data distributed across your on-premises private cloud, multiple cloud providers, and on AWS, you need an advanced data encryption solution. Vormetric Transparent Encryption protects your files and databases on your premises and across multiple clouds including AWS, without any changes to applications, databases, infrastructure or business practices.

Vormetric Transparent Encryption:

- Strengthens data security with operating system-level controls against unauthorized access based on granular access policies, including user identity (including for administrators with root privileges), and process, among many others
- Accelerates breach detection and satisfies compliance mandates with detailed file access logs, directed to your security information and event management (SIEM) system
- Delivers a fast return on investment with a non-intrusive, flexible implementation. Encryption agents operate on AWS EC2 compute instances or any other server accessing storage, protect EBS, EFS and S3 storage, and are available for many Windows versions and Linux distributions, including Amazon Linux

Centralized, secure key management

The Vormetric Data Security Manager centralizes key, policy and log management for Vormetric Transparent Encryption, available as a FIPS 140-2 Level 2 or 3 appliance or a FIPS 140-2 Level 1 virtual appliance. The physical appliance is appropriate for your on-premises locations to manage encryption agents worldwide across any cloud provider. The virtual appliance is available in many virtualization formats including VMware and KVM as well as an Amazon Web Services AMI and on the Microsoft Azure Marketplace.

Accelerated PCI-DSS compliance

Vormetric Tokenization with Dynamic Data Masking secures and anonymize sensitive assets in the data center, big data environments or the cloud for simplified PCI-DSS compliance. Format-preserving or random tokenization protects sensitive fields while maintaining database structure, for a non-disruptive implementation. Then, it's easy to add policy-based dynamic data masking to applications.

The Vormetric Tokenization Server is available as a shared AWS AMI.

AWS encryption key management

Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager.

The CipherTrust Cloud Key Manager leverages cloud provider Bring Your Own Key (BYOK) API's to reduce key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility. The solution is available as a shared AWS AMI, or can be deployed on premises or in any supported private cloud deployment to meet more stringent compliance requirements.

CipherTrust Cloud Key Manager offers the following advantages:

- Safer key management practices combined with cloud benefits of scale, cost and convenience
- Greater control over keys—you can control key generation and storage of keys used in AWS KMS, Microsoft Azure and more!
- Enhanced IT efficiency with multi-cloud key management from a single console that offers automated key rotation and comprehensive key life cycle management

Fulfill your data protection requirements

Thales simplifies securing Amazon Web Services workloads and helps achieve compliance with data security regulations. Vormetric Data Security Platform products operate seamlessly on workloads in AWS and on your premises delivering centralized policy and key management, and Thales multi-cloud key management brings you into compliance with best practices and data protection mandates.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.